
CYBERSECURITY CHALLENGES IN THE OFFSHORE OIL AND GAS INDUSTRY: AN INDUSTRIAL CYBER-PHYSICAL SYSTEMS (ICPS) PERSPECTIVE

Abubakar Sadiq Mohammed

School of Computer Science and Informatics
Cardiff University, UK
mohammedas@cardiff.ac.uk

Philipp Reinecke

School of Computer Science and Informatics
Cardiff University, UK
reinecke@cardiff.ac.uk

Pete Burnap

School of Computer Science and Informatics
Cardiff University, UK
burnapp@cardiff.ac.uk

Omer Rana

School of Computer Science and Informatics
Cardiff University, UK
ranaof@cardiff.ac.uk

Eirini Anthi

School of Computer Science and Informatics
Cardiff University, UK
anthies@cardiff.ac.uk

February 25, 2022

ABSTRACT

The offshore oil and gas industry has recently been going through a digitalisation drive, with use of ‘smart’ equipment using technologies like the Industrial Internet of Things (IIoT) and Industrial Cyber-Physical Systems (ICPS). There has also been a corresponding increase in cyber attacks targeted at oil and gas companies. Oil production offshore is usually in remote locations, requiring remote access and control. This is achieved by integrating ICPS, Supervisory, Control and Data Acquisition (SCADA) systems, and IIoT technologies. A successful cyber attack against an oil and gas offshore asset could have a devastating impact on the environment, marine ecosystem and safety of personnel. Any disruption to the world’s supply of oil and gas (O&G) can also have an effect on oil prices and in turn, the global economy. This makes it important to secure the industry against cyber threats. We describe the potential cyberattack surface within the oil and gas industry, discussing emerging trends in the offshore sub-sector, and provide a timeline of known cyberattacks. We also present a case study of a subsea control system architecture typically used in offshore oil and gas operations and highlight potential vulnerabilities affecting the components of the system. This study is the first to provide a detailed analysis on the attack vectors in a subsea control system and is crucial to understanding key vulnerabilities, primarily to implement efficient mitigation methods that safeguard the safety of personnel and the environment when using such systems.

Keywords Cyber security · Offshore oil and gas · Industrial Cyber-Physical Systems · SCADA · Cyber attacks

1 Introduction

Despite worldwide initiatives to implement green energy sources, the global demand for crude oil is expected to remain high for decades to come [1], [2]. This makes it ever more important to protect the industry from increasing cyber threats. While no business is immune to cyber security attacks, critical industries such as oil and gas (O&G) are

increasingly more vulnerable, with many hackers now targeting (directly or indirectly) the operational domain [3]. This is because Operational Technology (OT) and Industrial Control Systems (ICS) in the past had been physically isolated from outside networks [4] and based on proprietary hardware, software, and communications protocols [5]. This ensured that the only risk they were exposed to was within the scope of their operations locally [6] as many ICS components were in physically secured areas and the components were not connected to Information Technology (IT) networks or systems. However, due to the need to make faster and better business decisions, equipment are now smarter and are being integrated with multiple industrial technologies in IT in line with Industry 4.0 [7], sometimes referred to as "Oil and Gas 4.0" [8], [9]. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems [6]. As a result, the attack surface has widened with attacks growing in frequency over the last few years.

The integration of OT and IT has been aided by the rapid development of embedded systems, sensors, and networks, which in turn, has given rise to Cyber-Physical Systems (CPS) capable of advanced computing and networking technologies in a unified way [10]. Industrial Cyber-Physical System (ICPS) refers to CPS that is specifically designed for industrial applications [10]. This has opened the door to significant efficiency gains in the oil and gas industry [11] and is particularly the case in the offshore sector, where there is a pressing need to reduce costs and maximize equipment availability [11]. While it allows engineers to monitor and control assets remotely [7], [12], [13], this exposes ICS communication protocols to cyberspace vulnerabilities, like data exfiltration and malware injection attacks, which could cause significant losses to a company and potentially compromise process safety; endangering lives of personnel including damage to the environment. The migration to IT has also led to the standardization of new SCADA communication protocols such as Modbus-TCP Distributed Network Protocol (DNP3), IEC-60870-5-104 and the Inter-Control Center Protocol (ICCP, IEC60870-6) [12]. The first three were designed for automation and control, and the last was designed to connect SCADA systems [12]. Figure 1 shows an example of some typical components that make up an ICPS setup in an offshore O&G platform and highlights common vulnerabilities.

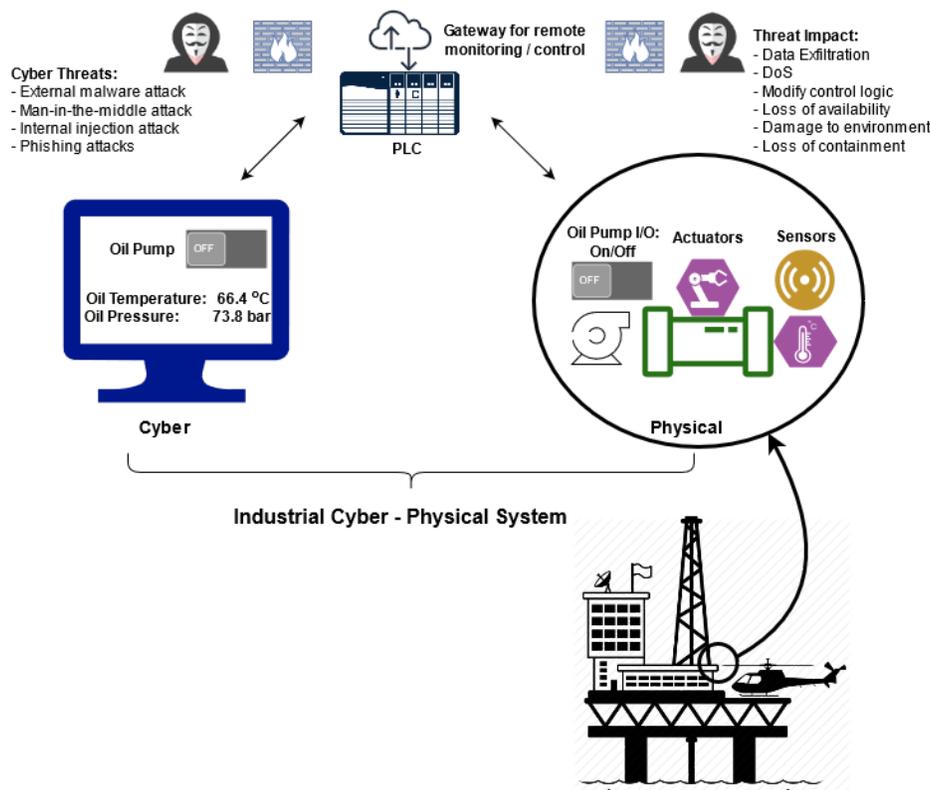


Figure 1: Example of a Cyber-Physical System in oil and gas highlighting common vulnerabilities

Being heavy industrial processes, O&G production and processing facilities rely heavily on ICPS [14]. Control equipment such as Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCS) are widely used, along with Human Machine Interfaces (HMIs) and Remote Terminal Units (RTUs) [14]. Using Industrial Internet of Things (IIoT) technology, the interconnection of these intelligent industrial devices with control and management

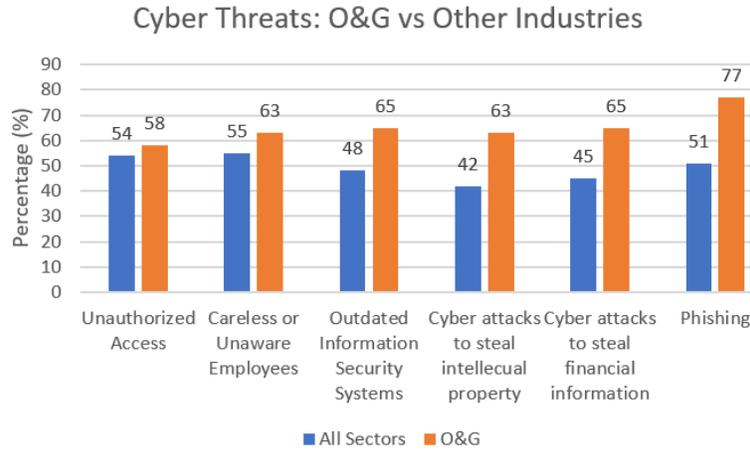


Figure 2: Cyber threats faced by O&G sector as compared to other industrial sectors. Source: EY Global Information Security Survey 2016-17 [20]

platforms, collectively improve the operational efficiency and productivity of industrial systems [15]. One of the more common use cases of ICPS in the O&G industry that depend on these control equipment is Asset Performance Management (APM) as it is a data-driven approach to asset management [11]. APM solutions are often linked to Computerized Maintenance Management Systems (CMMS) which also drives their deployment on-premise [11]. As the move toward minimally manned facilities continues, having remote visibility into operations becomes increasingly important [11]. Currently, the need to transfer production data to information systems, which also includes the needs for remote maintenance [14] has helped in broadening the attack surface across the O&G industry.

Due to their remote location in deep waters and the need for real time monitoring and control, offshore O&G assets, have potentially a wider attack surface compared to other sub-sectors of the industry, which makes them attractive to threat actors. This is critical because offshore production accounts for a significant proportion (about 30% [16]) of global O&G production. There also seems to be a passive shift in focus towards offshore production in some oil producing countries. In Nigeria, for example, some International Oil Companies (IOCs) are divesting their onshore producing assets to focus more on deep offshore production [17] [18]. In America, Equinor, which has a large portfolio of offshore assets in the US Gulf of Mexico, has agreed to divest its onshore assets in the Bakken Field [19]. These trends indicate that the offshore O&G sub-sector is likely to retain or increase its share of global oil and gas production.

Successful cyber-attacks threaten the competitiveness of the global O&G industry, and the cost of future breaches will be much higher, whether to corporate assets, public infrastructure and safety, or the broader economy through energy prices [20]. Breaches can lead to lost production, raised health, safety, and environmental risk, costly damages claims, breach of insurance conditions, negative reputational impacts, and loss of licence to operate. Therefore, cybersecurity needs to be a consideration throughout the life-cycle of any project, especially across digital transition activity [21].

The reported percentages of acknowledged cyber attacks indicate the high threat for offshore oil and gas assets [9]. A cyber-attack on an O&G OT environment can have serious results beyond just financial losses including environmental damage, loss of human lives [20], data and information theft, direct manipulation of machinery [7], changes to inclination of entire oil rigs [7], [22] or pressurisation of pipelines [7], [23], [24].

1.1 O&G vs Other Critical Infrastructure Industries

In 2017, EY carried out a 2016-17 Global Information Security Survey shown in Figure 2 where selected companies were asked which threats and vulnerabilities have most increased their risk exposure over the last 12 months. In every single metric recorded, the O&G companies had a higher cyber-attack incidence occurring compared to other critical infrastructure industries. More specifically, in the United States, the Department of Homeland Security responded to more than 350 cyber attack incidents at US energy companies between 2011 and 2015 and identified nearly 900 security vulnerabilities within those energy companies - a figure that was higher than any other industry [14] [25].

Another study that examined the state of cybersecurity in the United States O&G industry was carried out by The Ponemon Institute [26] in 2017, where 377 individuals who were responsible for securing or overseeing cyber risk in the OT environment were surveyed. It was discovered that only 41% continuously monitor all infrastructure to prioritize

threats and attacks. An average of 46% of all cyber attacks in the OT environment go undetected, suggesting the need for investments in technologies that detect cyber threats to O&G operations [26].

The vulnerability of this sector was evident in May 2021, when one of the largest pipelines in the US which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down its 5,500 miles of pipelines for six days due to a cybersecurity attack [27]. Reports indicate that this was a ransomware attack that targeted the IT system, yet its repercussions were felt in OT operations as headline news reported panic, social disruption, and a crippling lack of fuel delivery [28].

1.2 Related Work

A number of publications have outlined potential attacks on SCADA systems conventionally used in the O&G industry. These are summarised in Table 1. Very few publications survey cybersecurity topics specifically for the O&G sector [7], although some papers [40], [41], [42] survey cybersecurity incidents related to the O&G industry [7]. Stergiopoulos et al. [7] were the first to develop a vulnerability taxonomy for ICPS specifically for the O&G sector. The concepts presented in the study are broadly applicable to the 3 sub-sectors in O&G: upstream, downstream and midstream. We extend their study by analysing the key components in a subsea control system – which are usually designed to different standards from onshore platforms due to the extreme conditions that exist in deep waters, and we highlight vulnerabilities of the system to cyber attacks. The research to date has focused generally on ICS security, which is broadly applicable to most sectors with only a few analysing real cyber security incidents that have taken place in the O&G sector. Studies on O&G ICPS security have lacked domain knowledge of a complete end-to-end process system, while highlighting vulnerabilities. This is important because showing vulnerabilities of specific existing engineering designs used in the field could lead to more resilient systems. From a literature review perspective, it is evident that the subject of cyber security for O&G assets is not widely studied[9]. Reports also indicate that the industry’s cyber maturity is relatively low, and O&G boards show very little understanding of cyber issues [43], [7]. As a result of the increase in cyber attacks on O&G ICPS and the lack of an understanding of the associated attack vectors in such systems, it is critical to investigate this further in order to ensure better protection of vulnerable assets.

1.3 Motivation

Out of 42 recorded cyber security incidents [7] affecting the O&G industry in the past decade, the upstream sector had the highest number of incidents. This gives an indication of a higher vulnerability in this sector compared to other O&G sub-sectors. Moreover, because the upstream sector is the first stage of 3 highly inter-connected sectors of the O&G industry (which will be described briefly in Section 2), any disruption will likely cascade down the value chain and have an impact on the other sectors. For these reasons, our paper will be focused on the upstream O&G sector. This work aims to answer key questions such as what unique challenges make the industry more vulnerable to attacks compared to others, and why the available datasets for cyber security research are largely not representative of the O&G industry processes. To the best of our knowledge, there has been no survey carried out specifically for the offshore environment of the O&G industry, identifying inherent vulnerabilities in an end-to-end subsea system. This paper aims to describe the oil and gas production process and its vulnerabilities, present a timeline of documented cyber attacks on O&G upstream assets, analyse a subsea control system architecture highlighting the vulnerabilities of the system to cyber attacks, and discuss limitations in available datasets for security research on OT infrastructure.

Our main contributions are: (i) A timeline of documented cyber attacks on O&G upstream assets; (ii) A case study of a subsea control system architecture highlighting the vulnerabilities of the system to cyber attacks; (iii) Mitigation strategies against cyber threats to subsea control systems. The remainder of this paper is structured as follows: Section 2 gives an overview of the upstream sector of the O&G industry and describes the oil and gas production process. Section 3 discusses common vulnerabilities, attack vectors in the sector, and a case study of a subsea control system architecture is presented. In Section 4, we explain challenges and analyse why upstream O&G assets are difficult to secure, while Section 5 looks at the state of securing O&G assets including datasets available for security research. Section 6 is the conclusion.

2 Overview of the Oil and Gas Industry

The O&G industry comprises of three sub-sectors - upstream, downstream, and midstream infrastructures [7]. These sectors are quite diverse in their roles within the value chain. The *upstream* sector deals with exploration, drilling, and production [7] - basically all activities involving the search for oil/gas, the recovery process, and production from reservoirs hundreds of feet underneath the Earth’s surface at very high pressures and temperatures. It comprises of offshore and onshore operations. The *downstream* sector focuses on distributing assets to consumers [7] and handles

Author/Reference	Summary	Multiple Sectors	O&G Specific
Alcaraz et al. [12]	Presented generic architectural components of critical infrastructure components and their vulnerabilities	✓	
Kim et al. [29]	Surveyed CPS research in multiple domains including hybrid systems, security, and real-time computing and outlined potential for CPS in several applications	✓	
Krotofil et al. [30]	Presented a survey on ICS security research including security controls to mitigate vulnerability of common ICS protocols.	✓	
Mo et al. [31]	Their survey highlighted information security and system-theory-based security approach to securing cyber-physical systems	✓	
Stergiopoulos et al. [7]	Presented an attack taxonomy and catalogue of cyber attacks on O&G assets		✓
McLaughlin et al. [32]	Presented an overview of ICS security assessment including the key principles of ICS operations.	✓	
Sadeghi et al. [33]	Authors examine security and privacy issues relating to IIoT with proposed mitigations	✓	
Stellios et al. [13]	Authors assessed the IIoT threat landscape by analysing representative attacks against IoT in a risk-like approach	✓	
Khan et al. [34]	Proposed IoT architecture specifically for the O&G industry to aid functional and business requirements. The alternate architecture was based on three modules applicable to the upstream, midstream, and downstream sectors		✓
Sayegh et al. [35]	Authors presented a testbed used to detect vulnerabilities in SCADA protocols to internal attacks.	✓	
Nazir et al. [36]	Authors survey tools and techniques to discover SCADA system vulnerabilities common to CPS deployed in numerous sectors	✓	
Bhamare et al. [37]	Explored major publications from industry and academia and addressed applicability of machine learning techniques for ICS cybersecurity	✓	
Miller et al. [38]	Authors analysed cyber security incidents on critical infrastructure and SCADA systems and developed a taxonomy to classify future SCADA security incidents	✓	
Giraldo et al. [39]	Authors lay out a classification in CPS domains, security level implementation, and computational strategies from a survey of numerous surveys	✓	

Table 1: Summary of Related Work

the refining of the natural gas or crude oil produced and its storage facilities (oil refineries, Liquefied Natural Gas plants, gas stations, petrochemical plants, etc) while the *midstream* connects the upstream activities to the downstream activities [7] (transportation – pipelines, crude oil tankers, trucks; and some marketing activities). These three sectors are interconnected and interact through a complex web of activities which are streamlined to ensure a timely and safe delivery of petroleum products to the end consumers. These sectors are highlighted in Figure 3. In the next sub-sections we will describe the life cycle of an O&G upstream asset and the oil and gas production process.

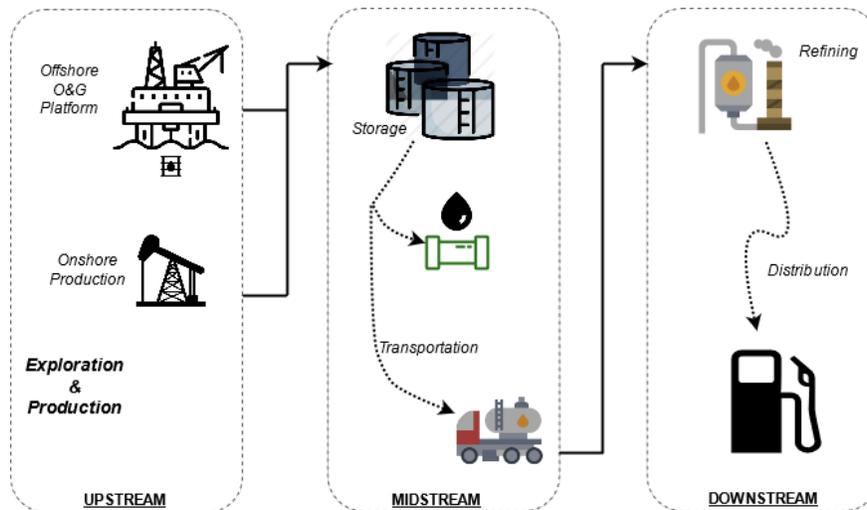


Figure 3: Oil and Gas Value Chain

2.1 Life Cycle of the Upstream Oil and Gas Industry

Upstream activities include exploration, drilling, and production and are typically referred to as E&P (Exploration & production). More specifically, the upstream life cycle is split into five phases which cover the 'cradle to grave' activities ranging from how the hydrocarbons are discovered to reservoir depletion, and decommissioning (returning the environment to its pre-E&P state). The activities that take place in each phase and their average timelines are summarised in Table 2.

Phase	Timing	Activities
1. Exploration	1-5 years	Exploration for potentially viable oil and gas sources through geological surveys. Often no potentially viable oil and gas sources are discovered and operations are terminated [44].
2. Appraisal	4-5 years	Sites identified as potentially containing viable oil/gas sources are examined in more detail [44].
3. Development	4-10 years	Limited infrastructure and site development will already be in place as part of the exploratory and initial drilling phase, but during the field development phase activity will dramatically increase and first oil/gas will be produced towards the end of this phase [44].
4. Production	20-50 years	Oil/gas reserves are being extracted and transported for processing and distribution [44].
5. Decommissioning	2-10 years	Usually during decommissioning, the platform is completely removed and the seafloor returned to its unobstructed pre-lease condition [45]. Once it is no longer cost-effective to extract remaining reserves, the site is decommissioned and the operating companies are typically responsible for returning the site to as close to original state as possible [44].

Table 2: Upstream life cycle describing activities carried out during each phase

2.2 Upstream O&G Production and Processing

Oil and gas production is the process of extracting reservoir fluids (hydrocarbons) from beneath the earth's surface – typically at high pressures and temperatures, and separating the mixture of oil, gas, and water at the surface. The main activities are gathering (from wellheads to separators), separations (separate oil, gas, and water), gas compression (prepare for storage and transport), temporary oil storage, waste water disposal, and metering (calculation of quantity before export) [46]. From the wellheads, reservoir fluids are fed into production and test manifolds. Next stage is the separation process, where horizontal gravity separators are usually used [47] in most facilities. The fluids are separated based on their densities (water is heavier than oil while gas is the lightest). In the separator, the pressure is often reduced in several stages - from high pressure to low pressure - to allow controlled separation of volatile components [47]. The gas is dehydrated, compressed and used to power the plant in most cases while the rest is exported. The oil is also processed and stored in settling tanks ready for export while the produced water could be re-injected into the reservoir for pressure maintenance or disposed of safely. There are a number of variations to this process depending on the crude oil composition and the required end products, but this is the typical baseline setup for most oil and gas production facilities. This process is illustrated in Figure 4.

2.3 Offshore Operations

Offshore O&G operations are a subset of upstream operations. It is common for offshore O&G operators to have a service territory that spans a large geographic area [14]. A large O&G company operating offshore, for instance, generates, transmits, and stores petabytes of sensitive and competitive field data; and operates and shares thousands of drilling and production control systems spread across geographies, fields, vendors, service providers, and partners [48]. Most of the field data transmitted and stored are collected by sensors that are part of an industrial control system. ICPS sits at the heart of remote operations which enables the satellite platforms to be fully automated. For this reason, central operations centres may be constructed to control system flow and monitor system conditions [14], which is made possible by utilising ICPS for collection of data and control of critical system processes. A large offshore oilfield development project would typically have several types of platforms to effectively extract and export oil and gas resources from the deep oceans. These structures would be distributed around the field(s) (several kilometers apart) as satellite platforms. The reservoir fluids extracted would be transported via pipelines to a central processing facility (CPF) where they are processed, stored, then offloaded to export tankers. The extraction of crude oil from offshore facilities is made possible by subsea control systems, and in recent times subsea production systems. These are highly advanced equipment designed to operate under extreme pressures and temperatures found in deep waters.

Drilling Campaigns: Throughout the life of a field, there will be several drilling campaigns carried out. During the exploration phase, the aim of drilling is to find commercial quantities of hydrocarbons. In the appraisal phase, the aim of drilling is to confirm how large the reservoir is and its characteristics. Development phase drilling is more precise as this is where the initial production wells will be drilled. During production, however, there will still be some drilling campaigns - referred to as in-fill drilling. This is to improve the efficiency of depleting the reservoir by adding more wells during the life of the field. This is why there are usually drilling rigs moving between fields to execute drilling campaigns all over the world. When a drilling rig arrives on site, it can be attached to a host platform for shared resources. This is usually taken into account when designing offshore structures. Drilling operations are usually carried out by oil service companies. They are different from the company who owns and operates the asset. A common use case for ICPS during drilling operations is to enable leak detection, in which a remote multi-sensing technology [49] could be used. This helps in identifying potential leaks and aids quick response to limit the release of harmful hydrocarbons into the environment.

2.4 Emerging Trends - Remote Offshore O&G Production Operations

While most offshore platforms are still currently manned facilities, there seems to be a trend indicating a shift towards operating oil rigs completely remotely from land. Several recent studies and innovations supporting unmanned O&G production have also indicated this shift in thinking [50] [51] [52] [53] [54]. Some examples of such studies are the DNV GL's unmanned floating LNG (Liquified Natural Gas) concept, Solitude and Aker Solutions' conceptual idea for an unmanned FPSO with annual maintenance campaigns [55]. Equipment is modularized and monitored from shore with much of the routine maintenance and fault correction carried out by self-programming autonomous inspection and maintenance units [1]. With these developments, it is safe to conclude that the ability to operate an unmanned platform as part of a portfolio of offshore assets allows materially reduced OPEX [56]. This is a huge factor influencing O&G companies operating offshore to invest in this technology, which also has the potential to increase the attack vectors.

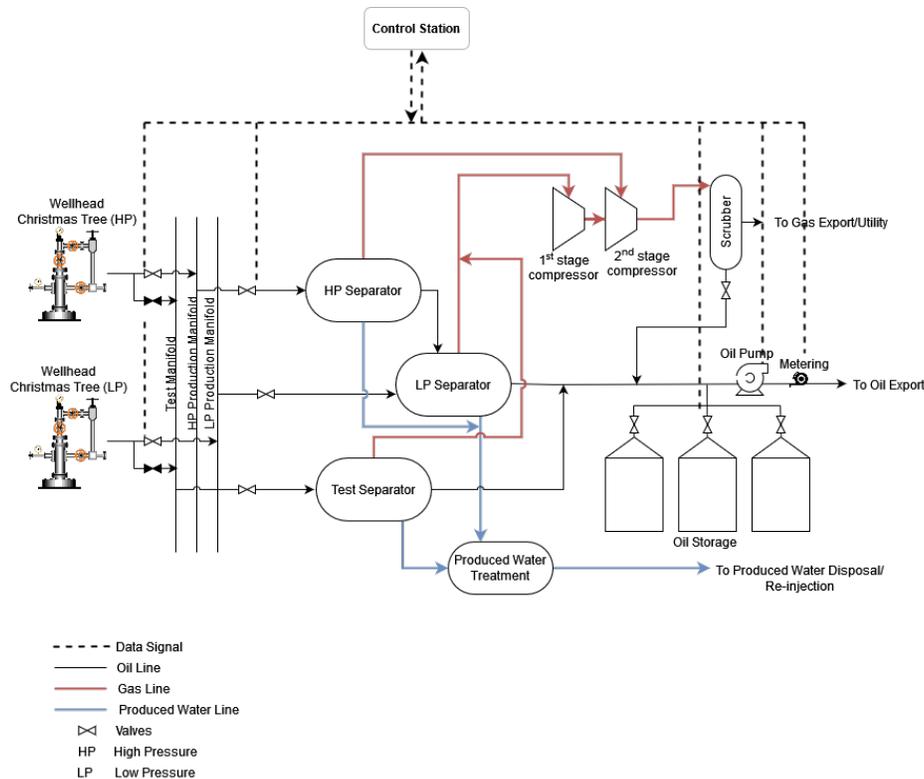


Figure 4: Upstream oil and gas production process

3 Common Vulnerabilities and Attack Vectors in the Upstream O&G Industry

In Section 2, the basic process flow in oil and gas production was described. There are inherent vulnerabilities that an attacker could exploit in the system. In this section, we will discuss the types of attacks that can compromise the system and present a case study of subsea control, communications, and its common vulnerabilities. Process monitoring and remote control are two common activities that utilise ICPS and automation to optimise operations. These are generally applicable to:

1. **Monitoring (Sensors):** Temperature, pressure, chemical composition, leak detection, etc.
2. **Remote Control:** Valves/actuators, pumps, hydraulic and pneumatic control systems, Safety Instrumented Systems (SIS), Emergency Shutdown Systems (ESD), Fire & Gas Systems (F&G), High Integrity Pressure Protection System (HIPPS), etc.

The following sub-section will examine the attacks that could compromise any of these listed operations.

3.1 Types of Attacks

- **Denial of Service (DoS):** One of the main safety features for process control are Emergency ShutDown systems (ESD) which are used to prevent unsafe operating conditions. In a DoS attack, an attacker could take advantage of vulnerabilities in data signal like insecure communication protocols not requiring authentication, and flood the network with random commands which effectively renders the ESD incapable of responding to unsafe process control requests. If an attacker, for example, were to carry out a DoS attack on the ESD of an unmanned offshore oil facility, a major catastrophic event could happen if there was a pressure build-up in the crude oil export lines. This kind of attack ensures that the onshore control centre loses its ability to shut down critical process to avert danger.
- **Oil Tank Level Spoofing Attack:** Processed oil that has been treated and separated from gas and water is stored in settling tanks ready for export. These tanks are fitted with level control sensors that transmit information to prevent tank overfills. The main goal of this attack is to falsify sensor readings indicating that

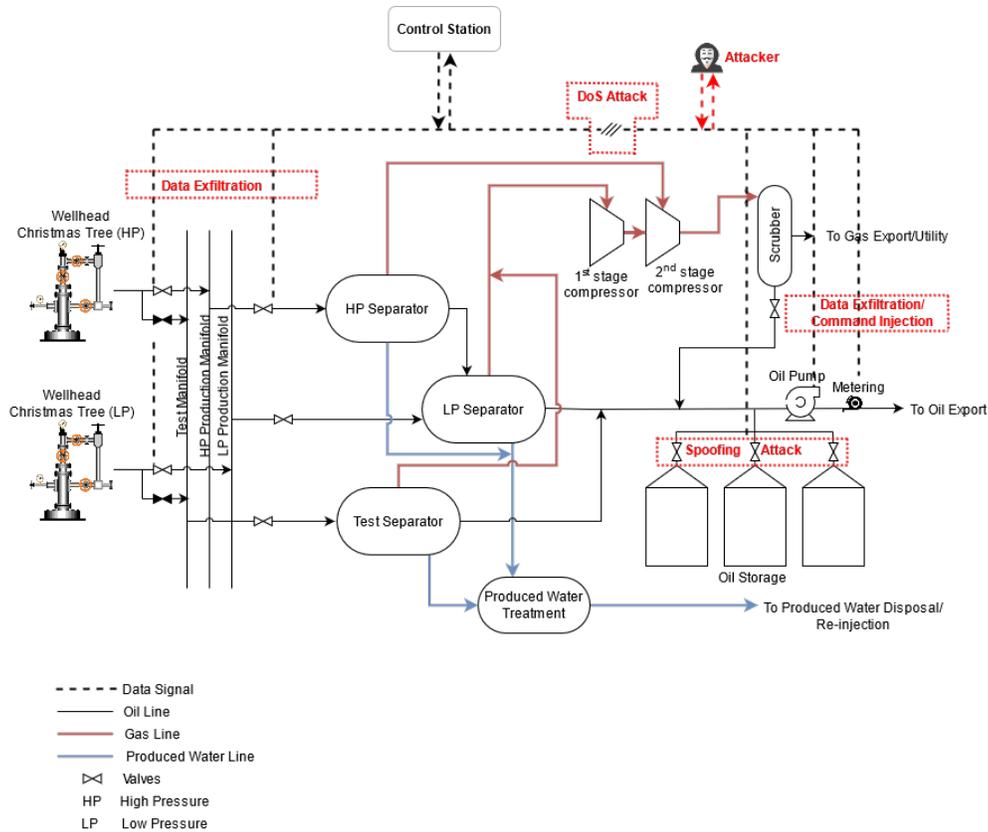


Figure 5: Upstream oil and gas production process showing potential cyber attacks

the tank level is lower than it actually is, which could lead to explosions due to a tank overflow as oil is a highly volatile product.

- **Wellhead Production Data Exfiltration:** By discretely deploying malicious software such as trojans on compromised workstations in the control station, an attacker could be privy to sensitive information like wellhead production data. There are various ways a threat actor could harvest sensitive company data they are all stealthy techniques. An example is with the use of Domain Generation Algorithms (DGA) in establishing communications between bots and their Command-and-Control (C&C) servers. Accessing metering data at custody transfer points also avails an attacker with sensitive information. This could allow threat actors to study hydrocarbon export volumes over time and arm them with enough information to prepare stealthy spoofing attacks that could cause loss of revenue to the company. Some companies have had their data discretely exfiltrated for years before it was found out.
- **Command Injection:** PLCs control numerous operations in the oil production process described earlier in Figure 4. An example is the oil export system which comprises of export pumps, flow computers, flow meters, and actuators. If an attacker were to compromise an engineering workstation in the control centre, they could alter commands to cause the pump or actuators to perform inappropriately. In addition, PLCs are programmed to control the process to perform within safe operational parameters like maximum allowable pressure and flowrate. These set point limits, if tampered could lead to unsafe operational states. Oil and gas, being volatile products, need very little instability to ignite and cause explosions.
- **Data Tampering:** Processed data could be tampered with by an attacker. An attacker could obfuscate the details of a wider attack by altering operation log and system control-related data [57], which would deceive defenders carrying out a post-attack forensic analysis. Data historians in offshore control stations that store operation log files could be targeted by this attack.
- **Choke Size Replay Attack:** In this attack, the signed packets sent over the network could be captured and resent multiple times to the destination [58]. An example of a dangerous application is if an attacker were to intercept commands sent to increase or decrease the choke size of a well (to increase or decrease crude

O&G Process	Attacker Motive	Potential Attack	Component	Consequence	Impact
Oil tank storage	Service disruption	Spoofing	Level sensors	Tank overfill, loss of containment	Explosion, loss of life, environmental damage
Hydrocarbon separation	Revenue loss	Data tampering	Pressure or Temperature sensors	Incomplete separation of gas from oil	low quality product, loss of revenue
Oil delivery, export, piping	Service disruption	Command injection	PLC, pumps, actuators	Operations outside allowable limits	Potential damage to asset and environment, potential loss of lives
Emergency Shutdown	Damage to asset	DoS	Safety Instrumented System, PLC, and actuators	Operations outside allowable limits	Potential damage to asset and environment, potential loss of lives
Custody Transfer/metering	Revenue loss, theft of operational information	Data exfiltration	flow computers, meters, pressure/temperature sensors	Incorrect calculation of hydrocarbon volumes, sensitive operational data leakage	Loss of revenue, reputational damage

Table 3: Attacks on some O&G upstream processes showing attacker motives and impact

oil production rates). They could replay these commands to increase the choke size, masking as a legitimate command, which could damage the reservoir permanently.

Table 3 summarises some of these potential attacks on upstream O&G processes showing attacks, attacker motives, vulnerable components, and potential consequences including impact of attack. These vulnerable points in the oil production process are also highlighted in Figure 5.

Based on the recorded security incidents [7] affecting upstream O&G assets, Figure 6 shows a pattern that indicates that these vulnerabilities are already being exploited, and that threat actors have this capability. The most frequent impact from these attacks were theft of operational information (8 incidents), Denial of Service (6 incidents), modification of control logic (6 incidents), and change of program state (6 incidents). The impact of these types of attacks on a subsea control system are investigated in sub-section 3.2.

3.2 Subsea Control and Remote Monitoring - A Case Study

One of the critical processes in offshore operations is the subsea control system. Located hundreds of kilometres under deep waters, this system is essentially responsible for real time monitoring of production parameters to prevent unsafe conditions. We have focused on an offshore system because, as discussed earlier, records indicate that the upstream sub-sector is more vulnerable to attacks. Furthermore, an attack on a physical process in an offshore (possibly unmanned) asset will take a much longer time to respond to, compared to an onshore asset, given that it is located hundreds of kilometres in the oceans - which increases the likelihood of devastating impact. An example of a typical setup is shown in Figure 7 where production is monitored via HMIs at the Master Control Station (MCS) and remote workstations that could be located further away in onshore offices. The functions of these components are described in Table 4. A subsea control system comprises of one or more of the following components [59]:

- a wellhead with connected casing strings;
- a subsea christmas tree comprising pressure and flow control valves;
- a production control and monitoring system for remote monitoring and control of various subsea equipment, possibly multi-phase flow meters;
- a chemical injection system;
- an umbilical cable with electrical power and signal cables, as well as conduits for hydraulic control fluid and various chemicals to be injected into the produced fluid streams.

The components in the subsea architecture can be split into the following layers [7]:

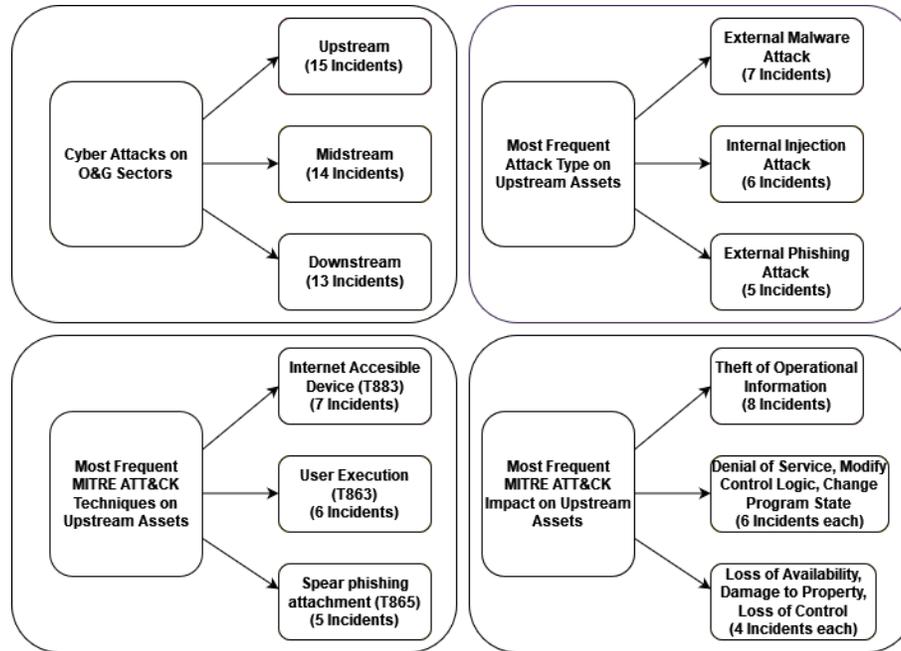


Figure 6: Analysis of cyber attacks on upstream assets [7]

Component	Function
Wellhead Christmas Tree	Combines with wellhead to constitute the pressure barrier between reservoir and environment and allow for control of well through various valves and sensors
Subsea Electronic Module (SEM)	Collects sensor data from wellhead interfaces
Subsea Control Module (SCM)	Houses the SEM and control valve module
Umbilical Cable	Houses a collection of hydraulic, data (fibre optic), power cables
Master Control Station (MCS)	Main field control station where HMIs and servers are located for logging and processing real time system data
Topside Junction Box	Combines all electric and hydraulic power generated topside and transmits to subsea network (umbilical termination unit)
Hydraulic Power Unit (HPU)	Power source for hydraulics to move valve actuators
Electrical Power Unit (EPU)	Power source for electrical components

Table 4: Functions of Some Components of a Subsea Control System

1. **Hardware:** Sensors, actuators, RTUs, PLCs, server equipment (racks, CPUs), routers, access control hardware (smart cards, RFID, etc), and valves.
2. **Firmware:** Operating systems, data and instructions for controlling the hardware.
3. **Software:** HMIs, Application Programming Interface (APIs), proprietary software packages, and applications.
4. **Network:** Communications protocols, modems/routers, firewalls
5. **Process:** Designed ICS business logic, control systems configuration

3.2.1 Attack Vectors of Subsea Control Systems

1. **Interception of Commands and Sensor Readings:** The initial stages of an attack requires gathering information on the system and operating parameters. This could be executed with a Man-in-The-Middle (MiTM) attack, where the connection between source and destination ports is intercepted, creating two new channels of communication: one connection between the source device and attacker, and another one between the attacker and the destination device [60]. This attack could compromise the software layer of the subsea architecture. Assuming an attacker managed to compromise a workstation within the MCS, they would gain access to the HMI and sensitive information like pressure and temperature values, production flowrates, maximum

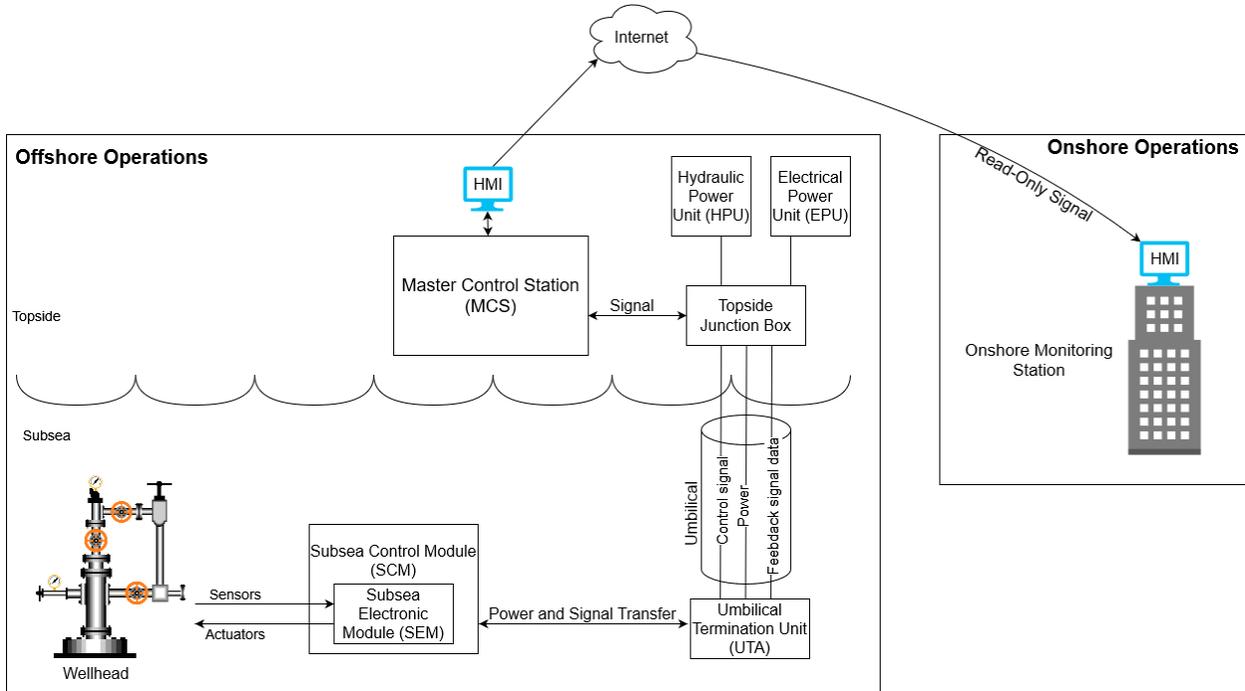


Figure 7: Example of an offshore subsea production monitoring system

allowable working pressure (MAWP), and valve fail-safe positions. Additionally, the attacker is able to act as a proxy and therefore read, insert, and modify data in the intercepted communication [60]. Earlier analysis has shown documented cyber attacks involving theft of operational information as indicated in figure 6. Adding authentication and encryption of data helps to defend against this kind of threat. Park and Kang [61] proposed a solution to MiTM attacks by authentication inter-device communication where each sensor is involved in the generation and distribution of session keys [58].

2. **Injecting Falsified Sensor Data:** The goal of this attack is to compromise the integrity of the sensor readings. This is a spoofing attack which is a variant of the MiTM attack where the attacker modifies data between two communicating devices. The firmware and hardware layers of the subsea architecture are susceptible to this kind of attack. An attacker intercepting communication between the SCM and the MCS conveying sensor readings could modify these values even before the gateways (serial-to-ethernet converters) convert the data to ethernet packets [62]. Another example is where an attacker, using the compromised workstation, manages to modify control logic of the SCM altering upper or lower limits of set pressure points which could cause a well blowout. The oil spill in the Gulf of Mexico in 2010 has shown how devastating the impact of a subsea well blowout can be to the environment [63] and safety of personnel. Figure 6 shows six incidents of documented cyber attacks each involving modification of control logic and changing program state which indicates that threat actors have this capability. A number of studies have suggested mitigation against this type of attack by using physics-based methods [64] which consider the effects of the attack on the controlled physical process and look for deviations from expected physical sensor measurements [65]. Azzam et al. [65] proposed an Early Warning System (EWS) that, on its own, is not capable of detecting injection of false sensor readings, but can generate early warnings in ICPS based on preliminary indicators. They applied their framework to Linear Time-Invariant (LTI) systems and adapted existing reachability analysis tools to compute a suspicion metric. This could prove useful if integrated with other intrusion detection capabilities to thwart stealthy malicious attempts.
3. **Denial of Service (DoS) Attack:** One of the most common attacks for cyber adversaries to conduct is the DoS attack [66]. System availability is of utmost importance in a subsea control system architecture and the attacker can flood the communicating device with requests to jam the communication channels and prevent legitimate requests [66]. DoS can compromise the network and hardware layers of the subsea control system and render engineers in the MCS incapable of sending emergency shutdown commands to shut-in wells discovered to be operating in unsafe conditions. Figure 6 shows documented cyber attack cases of DoS and loss of availability in six and four separate incidences affecting upstream O&G facilities respectively. DoS can have very serious

impact by disabling critical equipment in a subsea control system architecture. Sicari et al. [67] proposed a defence mechanism against different types of DoS attacks named REATO. They examined a cross-domain and flexible middleware, named NetwOrked Smart object (NOS) and tailored REATO to it.

The most common communication protocols being used in this setup are EthernetIP and Modbus. Availability of these systems is key and the communication of both control signals and sensor monitoring data are often not encrypted and not signed for data integrity [68]. With the growth in offshore E&P activities due to rising number of mature (depleted) onshore oilfields in recent years [69] subsea production is set to dominate a significant market share in the industry. The major vendors in the subsea control equipment market are Subsea 7, Technip FMC, Akastor ASA, Baker Hughes, and National-Oilwell Vargo Inc [69] while for DCS we have ABB, Emerson, Honeywell, Rockwell Automation, Schneider Electric, and Siemens [70] dominating the market share. In isolation, these equipment are robust and are safe for operations. However, in a bid to increase their market share, these key vendors controlling the market share are designing products with more and more integration with corporate IT systems which introduces more attack vectors with an increased risk of zero day attacks.

3.3 History of Cyber-Attacks on Upstream O&G Assets

A number of cases have been reported where upstream systems were directly or indirectly compromised by malicious insiders or malware, causing a number of adverse effects on operations and machinery [42], [7], [71]. Stergiopoulos et al. [7] catalogued 24 major cybersecurity attacks and events on upstream systems. We have used this information as a baseline to present a timeline of chronological security incidents that have affected the upstream O&G sector (see Figure 8). The temporal characteristic shows a growing frequency of data exfiltration attacks against upstream O&G production companies in recent times which could be indicative of the consequences of increasing integration of real time OT monitoring parameters with corporate IT networks to improve decision making. This is a part of the digital oilfield trend being witnessed in the industry. The O&G industry, in particular, is very competitive and almost any kind of leaked information can be beneficial to a competitor [68]. Obtaining sensitive data like well drilling techniques, data on suspected oil and gas reserves, and special recipes for premium products [68] including chemical injection and corrosion inhibitors can prove to be very valuable and therefore attractive to attackers.

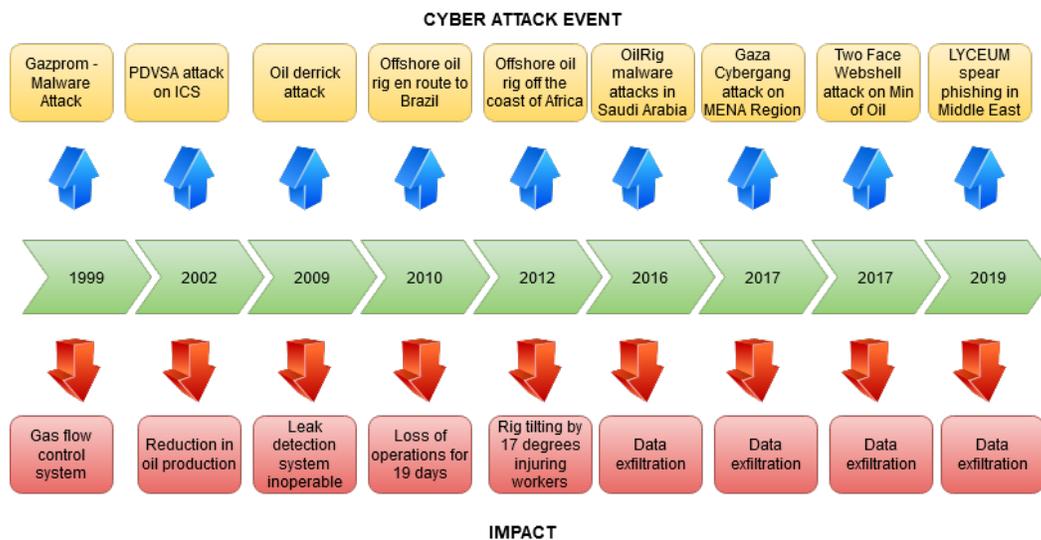


Figure 8: Timeline of Cyber Attacks on Upstream Oil and Gas Facilities [7]

3.4 Threat Actors and Motivation

Threat actors operating in this sector typically range from those looking for ransom to those operating for rivals within the industry or outside and last (but not the least) state sponsored agencies with specialised hackers at their disposal. The last category has immense resources and the potential to devastate critical infrastructure is massive [72] as seen in the case of Stuxnet - A virus that was reportedly designed by State intelligence to spy on and disrupt Iran's nuclear enrichment centrifuges, but also ended up spreading to infect Chevron facilities [73], a major O&G company.

They can generally be classified as [74] [75] [68]:

- **Disgruntled Ex-Employee:** Usually motivated by revenge on employer by triggering information disclosure to public to cause embarrassment, or to sell sensitive information. Person may still possess knowledge of sensitive information like passwords or system architecture.
- **Insider Threat (Disgruntled Employee):** Insider threat could also be motivated by revenge although there are several factors that could cause a person to turn against their employer. Defence against this kind of threat actor is very complex, as they have access to a lot of data.
- **Hacktivists:** This group is motivated by certain ideologies and will not hesitate to infiltrate a company they feel has gone against those principles. Their goals are usually to expose secrets and whistle-blowing.
- **Nation State Hackers:** These are hired by a Government to perform cyber operations against other nations. O&G producing nations usually rely on the revenue generated from oil production as a major source of economic power. This is what makes the impact of successful attacks to be significant to victim States. These groups are highly resourceful and aim to inflict maximum damage (loss of life and damage to environment).
- **Cyber Terrorists/Organised Crime:** Non-State hackers are groups or individuals with the main intention of obtaining money by stealing sensitive data or confidential information and either selling it or blackmailing the company into paying a ransom.

There are also some known adversaries that have been identified to be targeting the O&G sector. These include [14]:

- **XENOTIME:** This group has been known to target O&G companies in the United States and Europe since 2018 and have compromised several ICS vendors and manufacturers.
- **MANELLIUM:** Since 2013, this group has been targeting petrochemical companies.
- **CHRYSENE:** Involved in the 2012 Shamoon cyberattack at Saudi Aramco and remains active and evolving in more areas.
- **HEXANE:** Capabilities of this group is still being studied by Dragos but was first identified in 2019.
- **DYMALLOY:** A highly aggressive and capable activity group that has the ability to achieve long term and persistent access to IT and OT for intelligence collection and possible future disruption events.
- **APT33:** A group that has compromised oil companies in the United States, Europe, and Asia by obscuring a dozen live C&C (Command & Control) servers that have been used to do reconnaissance and botnet management since 2018 [68]. C&C connections to cloud services are difficult to detect since they use normal services that any employee could use for legitimate purposes [68].

In the next section, we will examine the unique challenges in the upstream O&G sub-sector that has made it attractive for these threat actors to actively carry out attacks on the targets discussed.

4 Challenges in securing upstream assets

There are some unique traits that make the upstream O&G sector more challenging to secure [14] [68] when compared to other critical infrastructure industries. These are highlighted as:

- Upstream assets are usually spread over huge geographical landscape, including significant assets offshore.
- Offshore assets are usually in remote locations and in deep waters.
- A large percentage of production facilities have been designed decades ago and lack modern security features which make them vulnerable and obvious targets for cyber attacks.
- The frequent integration of vendor systems with operating company systems.
- **Dependencies:** Large distances and deep waters make it costly to establish a computer network for offshore platforms. Frequent damage to fibre-optic cables on seabed make it challenging to establish redundant and completely independent network solutions.

Accuracy is also a big challenge in oil and gas as the exact amount/volumes of what is produced is not easily measured [46]. Hydrocarbon volumes fluctuate depending on environmental temperature and pressure conditions and require complex conversion calculations of the observed volumes at each custody transfer point [46]. It is possible to spoof this data in a way that will make it difficult to investigate [46]. Micro fractional changes to any one of the sensor parameters used in calculating hydrocarbon volumes over time could lead to significant losses to either operating companies or oil producing States. The latter could be better described as economic sabotage.

Process states and plant configurations are always changing, sometimes due to optimisations, but mostly as a result of degradation. An example is pressure vessels that have corroded beyond minimum thickness and can no longer withstand the Maximum Allowable Working Pressure (MAWP). Rather than outright replacement, vessels can be derated to a lower MAWP. This changes plant configuration and set point limits. Also, as discussed earlier, the life of a field in production may last up to 50 years, yet the assets have a design life considerably less than that - usually 25 years [76]. Life extension projects are carried out on facilities to extend, upgrade, and further optimise operations. This is why after a major maintenance phase, it is not unusual to have a system operating in a manner slightly different from prior to the maintenance activities. These configuration changes need to be taken into account when designing an efficient cyber security mitigation strategy.

The challenges in securing ICPS from cyber attacks in the offshore O&G industry can also be broadly grouped into operational, financial, and legislative.

Operational Challenges: Keeping OT running at all times is critical for any successful industrial plant: every second systems are offline can cost the operating company thousands of dollars and recovering from a single hour offline can take days [77]. It is not unusual to witness systems running without being patched for years because operations availability and system up time go above security within ICS environment [78]. In restarting production wells after a shut-in, producers must also weigh the cost and mechanical difficulty of restoring those wells back to pre-curtailed volumes [79] as the transfer of fluids back to the wellbore after production restoration is not usually very efficient or complete [80]. This creates a high risk scenario where after a significant shutdown, depending on the age of the well, previous production level may never be attained again. The industry is intolerant of frequent shutdowns and as a result, there aren't many opportunities for security updates and patches which are necessary as most of the offshore platforms are legacy systems. There is a high number of old offshore platforms still producing today. In fact, nine of the world's longest-standing fixed offshore platforms are located in the North Sea, while one is in the Gulf of Mexico, US [81]. One of the oldest of them is a platform called Ekofisk 2/4 B, operated by ConocoPhillips and located 2.3km north of the Ekofisk Complex in the North Sea and it has been operating since 1974! To keep these platforms running efficiently, the operators retrofit new technologies onto legacy systems. This is usually done without security considerations that would adequately protect these systems from cyber attacks.

As discussed earlier, drilling campaigns are undertaken throughout the life of a field. Whenever a service company is contracted to drill wells for an operating company, this requires the use of shared computer networks, resulting in production equipment being exposed to network-related vulnerabilities [14]. The frequent integration of vendor systems with operating company systems is another risk factor that increases the attack surface of O&G production platforms. There is a need to ensure all sub-contractors keep the same or a higher level of cyber-hygiene than the operating company.

Financial Challenges: The offshore O&G industry is a highly regulated and capital intensive industry [2]. For example, FPSOs (Floating, Production, Storage, and Offloading vessels), because they give operators the freedom and versatility to explore remote areas and extract at a significantly cheaper cost [82], have become very popular in exploring deep offshore. The cost of a typical FPSO could range from \$800 million USD (Exxon Mobil's Kizomba A [83]) to \$3 billion USD (Total Nigeria's Egina FPSO [84]). The upstream life cycle discussed earlier shows that the company bears these huge costs for a number of years (during the exploration, appraisal, and development phases) before production begins, and thus are trying to recoup huge investments made as quickly as possible during the production phase. In turn, the production phase is the most vulnerable to cyber attacks, but the company's focus during this phase is on trying to break even, turning a healthy profit before the reservoir is depleted (limited period), and meeting their obligations to the host Government through payment of taxes and royalties. To achieve this, continuous operations with minimal shutdowns is usually prioritised over security concerns.

Legislative Challenges: Several governments all over the world have recognised the threat that cybersecurity poses the critical infrastructure industry. Even though it is usually the norm that each individual company bears direct responsibility over securing its digital systems, severe cyber attacks will have national implications as well [85]. This means that governments and the relevant agencies have a role to play in detecting, preventing and responding to such attacks [85]. A seamless transition between private sector companies to authorities will require a holistic threat picture, clear areas of responsibilities, and good procedures that are exercised regularly. This is hardly the case today [85]. In the United States, for example, There are stricter cybersecurity regulations that govern power, chemical, and nuclear facilities, but no federal laws impose such standards on the O&G industry [14]. O&G companies are not required to report cyber incidents, and as a result, the specifics are usually kept secret because companies tend to disclose information in exchange for anonymity [14]. This ensures that lessons learned from cyberattacks in one company and security measures implemented in response to such attacks are not always passed on to other companies in the sector, creating a serious knowledge gap [14]. Attacks are getting more sophisticated and government legislation is playing

catch up. There needs to be a concerted effort to create a legislative framework that ensures a minimum requirement for companies to secure their critical infrastructure assets from cyber attacks.

We have highlighted the financial and legislative challenges here to give context to the bigger industry problem, however neither are within the scope of this paper, as we have only focused on the operational challenges so far. In the next section, we will look at some general mitigation strategies, and how current datasets available to OT security researchers are inadequate for the o&G industry.

5 Securing Upstream O&G Assets - Current State

5.1 General Mitigation Strategies

General cyber security safeguards such as restricted physical access, cryptography, patch management, separation of corporate and production systems (through Demilitarized Zones (DMZ), Firewalls and Access Control Lists (ACLs)), and activity logging are all applicable mitigation strategies, but need to be viewed in conjunction with typical SCADA systems characteristics [36]. Although very little has focused on O&G assets, in the broader context there are some practical applications that can improve the cyber hygiene of upstream assets. Esfahani et al. [86] and Srinivas et al. [87] are both studies that proposed the use of lightweight authentication to ensure only authorised users gain access. In [86], a Machine-to-Machine (M2M) protocol based on hash and XOR operations was applied in two phases - (a) the registration phase, where each smart sensor registers itself to an authentication server with replication of pre-shared keys with the router, and (b) the authentication phase where mutual authentication is achieved between the sensor and the router [58]. [87] was based on chaotic map for IIoT environments which allows access to designated IoT devices only to authorised users with the use of personal biometric, smart cards, and passwords.

Research on ensuring basic security or defending against dreadful attacks in IIoT is still in its infancy [58] especially for the O&G sector, however, in the next sub-section, we shall examine intrusion detection systems and the limitation of datasets available to expand security research in this area that is applicable to the sector.

5.2 Intrusion Detection Systems (IDS)

Early warning and detection of breaches are essential for being in a state of readiness [72]. A number of systems have been designed to build threat detection capability in various industries, but only a few specifically for the O&G industry. Amongst these, Al-Issa et al. [88] suggested using Network Behavior Anomaly Detection (NBAD) and Network Data Leak Prevention (NDLP) Systems to help detect unusual behaviours in O&G facility systems and networks and detect the leak of information between the industrial control systems and the enterprise network respectively. Aljubran et al. [89] also proposed three useful tools that could, at best, provide a partial solution to the cybersecurity threat faced by remote offshore oil facilities. These are Safety Instrumented Systems (SIS), decision tree, and risk management.

The recent trend for the vast majority of research on Intrusion Detection Systems (IDS) is by application of machine learning techniques in developing an IDS for ICS [37]. Lack of adequate datasets remains the biggest hindrance to security research in this area is the. Machine learning (ML) has been used for identification of anomalous behaviours in industrial and manufacturing systems [90]. A ML-based firewall suggested by Haghghi et al. [91] towards securing ICS was focused on accuracy and achieving zero false-positives in developed classifiers. In another example, Anthi et al. [92] explored how adversarial attacks can be used to target supervised classifiers by presenting generated adversarial DoS samples to a trained model and understanding their classification behaviours on IoT devices.

Bhamare et al. extensively reviewed related works in the field of securing ICS/SCADA from cyber threats using machine learning which is summarised in Table 5 [37]. The studies were however limited in the scope of application as most were from specific industry data sets or limited simulated models of ICS that are not applicable to the O&G industry. A summary of this is shown in Table 6.

While contemporary IDSs use machine learning algorithms for pattern recognition to detect threat activities that are anomalous for a particular system, there are other IDSs which use signature-based systems to compare the activities to a database of known threats [97], [99], [94], [37]. Both of these methods can be combined to develop a robust detection system [37].

Zeng et al. [108] introduced a taxonomy of detection approach and also discussed machine learning-based solutions along with other types of available approaches for IDSs deployed in ICS [108] [37]. By their own admission, the authors confirmed that from the papers they surveyed, power systems are the main field that investigators study in [108].

Authors	Reference	ML Model and Implementation
Wehenkel	[93]	Decision tree induction, multilayer perceptron and nearest neighbour classifiers
Dua and Du	[94]	Cybersecurity using ML and data mining in general
Cardenas et al.	[95]	Attack categorisation, IDS
Zhang et al.	[96]	Support Vector Machine (S2 OCSVM), IDS
Yasakethu and Jiang	[97]	Artificial Neural Network, Support Vector Machine, Hidden Markov Model
Beaver et al.	[98]	Anomaly detection in SCADA via comparison of various ML algorithms
Maglaras and Jiang	[99]	One class Support Vector Machine, IDS
Hink et al.	[100]	OneR, NNge (Nearest Neighbour-like algorithm), Random Forests, Naive Bayes, SVM, JRipper, Adaboost
Erez and Wool	[101]	Single window classification algorithm deployed on IDS to detect irregular changes in SCADA control register values
Franc et al.	[102]	A Multiple Instance Learning algorithm used on network logs for security
Nader et al.	[103]	ML techniques with kernel methods to detect cyber attacks in water distribution systems
leahy et al.	[104]	Classification ML techniques
Valdes et al.	[105]	Unsupervised ML methods for anomaly detection in electrical substation circuits
Stefanidis and Voyiatzis	[106]	Hidden Markov Model, IDS
Bartos et al.	[107]	Support Vector Machine-based classification system

Table 5: ICS/SCADA Cybersecurity: Summary of Machine Learning Approaches [37]

ML Technique	Authors	Domain Secured
SVM/OCSVM	[98] [109] [110] [111] [97] [112] [99]	integrity, availability, confidentiality
Naive Bayes	[113] [98]	integrity, confidentiality
Decision Trees/Random Forests	[98] [113] [114]	integrity, confidentiality
Deep Belief Network	[109] [110]	availability, integrity
Artificial Neural Network	[109] [97]	integrity
KNN/K-means	[115] [116]	authentication, confidentiality, availability, integrity

Table 6: Popular ML techniques used in ICS Security

From their comparison, most of the datasets or testbeds utilised were from power grids and a small percentage from water distribution systems.

Challenges in the way of utilising machine learning and how it can help in defence mechanisms with respect to the relevant threats in ICS have been reviewed comprehensively by Zolanvari et al. [117], [37]. A case study was also presented where a ML-based IDS was developed using a SCADA testbed. The dataset from the testbed was deliberately built to be imbalanced by making the percentage of attack traffic in the dataset less than 0.2%.

A comparative analysis of various ICS datasets, summarised in Table 7, was carried out by Choi et al. [118]. The analysis seems to agree with our observed limitations of the current datasets used to conduct ICS security research and highlights why most are not applicable to a broad set of scenarios. For our case specifically (O&G offshore industry), most of the datasets do not account for the dynamic behaviour of monitored variables identified earlier. Pressure and temperature values change throughout the life of a producing field as the reservoir is being depleted which result in different hydrocarbon volumes calculated at any point in time. The monitored variables in current datasets only fluctuate within a given range. This is summarised in Table 8.

The review of existing literature shows that although a lot of research has been conducted on IDS security, the common limitation has been the availability of a wide scope dataset that applies to several critical infrastructure industries. The power industry is the most represented sector while an opportunity exists to create new datasets that represents commonly deployed ICS setup in the O&G industry.

ICS Dataset	Protocols	System	Year of re-lease	Data-type	Reference
Morris et al.	Modbus	Power, water, gas	2013, 2014, 2015, 2017	csv, arff	[119]
Lemay	Modbus	SCADA sandbox	2016	csv, pcap	[120]
SWaT	Modbus, Ethernet/IP	Water treatment	2016	csv	[121]
Rodofile et al.	S7Comm	Mining refinery	2017	csv, pcap	[122]
4SICS	Modbus, S7Comms, DNP3, Ethernet/IP	Complex	2015	pcap	[123]
S4x15 ICS Village CTF	Modbus	Complex	2015	pcap	[124]
DEFCON 23 ICS Village	Modbus	Complex	2015	pcap	[125]

Table 7: Summary of ICS datasets publicly available [118]

ICS Dataset	Num. of Pkts	Byte of Pkts	Duration	Data Capture		
				Continuous	Interruptions	Dynamic Variables
Lemay	2,588,491	169,690,458	15 hours	No	Yes	No
SWaT	19,761,714	5,498,545,489	11 days	Yes	No	No
Rodofile	23,387,064	5,848,801,728	27 hours	Yes	No	No
4SICS	3,773,984	314,562,089	1d 22 h 7 m	Yes	No	No
S4x15CTF DEF- CON23	1,678,668	124,271,095	N/A	Yes	No	No

Table 8: ICS datasets: Data capture summary

5.3 Overcoming the Challenge of Insufficient Research Data

Typically, industrial control systems manage critical industries (oil and gas, water, power, and chemical industries) that are sensitive to downtime. The risk of carrying out penetration tests on live operational equipment in the field to validate intrusion detection systems or other measures to improve the cybersecurity of such facilities is too high and can potentially cause damage or lead to loss of lives. Testbeds are the preferred methods for emulating ICS and deploying cyber threat detection/protection models on. However, the working philosophy and behaviour of different industry verticals is different. To design and develop the industry-specific best fit solution requires testbed of each type [126]. This will help in creating varied datasets that include industry-specific scenarios combined with machine learning models that are trained on benign and malicious activities which could improve the security posture of the industry.

6 Conclusion

This paper reviewed the growing threat of cyber attacks to ICPS in the offshore O&G industry as a result of the advancements in technology, digitalisation and integration of oil field equipment with corporate networks, and the need for remote monitoring and control. This has increased the attack surface available for cyber attackers to exploit. A timeline of documented cyber attacks on upstream O&G assets was presented which showed that data exfiltration has become more common in recent times, coinciding with the increase in integration of OT equipment with IT networks that is now prevalent in the industry. Furthermore, we gave a brief description of offshore O&G operations and the oil and gas production process, highlighting the possible areas of cyber attack infiltration.

We analysed a typical subsea control system architecture and highlighted its vulnerabilities to MiTM, DoS, and spoofing attacks by mapping the attacks to one or more layers of the architecture. Correlating these to documented cyber security incidents that affected the upstream O&G industry in recent times showed that threat actors have the capability to breach subsea control systems in its current state. We also discussed challenges in securing upstream assets, highlighting dynamic process state changes due to operations like derating of pressure vessels and asset life extension projects

which add to the complexity of identifying whether a changed plant configuration is legitimate or due to malicious actors. Mitigating strategies were also highlighted involving the use of IDS. There remains a lack of adequate datasets representative of processes in upstream oil and gas production.

6.1 Future Directions

Looking at the shift in philosophy of offshore installations from manned to unmanned facilities to be controlled remotely, and the current research into designing several of such, we can safely deduce that there will be an increase in digitalisation of offshore oilfields. With ICPS and IIoT improving integration of OT and IT there will be lots of opportunities for studies discovering new vulnerabilities in new systems. However, there is a need to create new datasets that also cater for the dynamic measurements and sensor readings of the offshore O&G industry. This shows that ICPS security in the O&G sector will continue to be a well researched area for the foreseeable future.

References

- [1] DNV GL. Oil and gas forecast to 2050, 2017.
- [2] Thumeera R Wanasinghe, Raymond G Gosine, Lesley Anne James, George KI Mann, Oscar de Silva, and Peter J Warrian. The internet of things in the oil and gas industry: A systematic review. *IEEE Internet of Things Journal*, 2020.
- [3] Giovanni Buizza Avanzini, Andrea Spessa, et al. Cybersecurity verification approach for the oil & gas industry. In *Offshore Mediterranean Conference and Exhibition*. Offshore Mediterranean Conference, 2019.
- [4] Dorothy Bundi and Mayieka Jared Maranga. Effects of cybercrime on oil and gas industry. *GSI*, 8(6), 2020.
- [5] Zakarya Drias, Ahmed Serhrouchni, and Olivier Vogel. Analysis of cyber security for industrial control systems. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–8. IEEE, 2015.
- [6] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.
- [7] George Stergiopoulos, Dimitris A Gritzalis, and Evangelos Limnaios. Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns. *IEEE Access*, 8:128440–128475, 2020.
- [8] Hongfang Lu, Lijun Guo, Mohammadamin Azimi, and Kun Huang. Oil and gas 4.0 era: A systematic review and outlook. *Computers in Industry*, 111:68–90, 2019.
- [9] Iosif Progoulakis, Nikitas Nikitakos, Paul Rohmeyer, Barry Bunin, Dimitrios Dalaklis, and Stavros Karamperidis. Perspectives on cyber security for offshore oil and gas assets. *Journal of Marine Science and Engineering*, 9(2):112, 2021.
- [10] Hakan Kayan, Matthew Nunes, Omer Rana, Pete Burnap, and Charith Perera. Cybersecurity of industrial cyber-physical systems: A review. *arXiv preprint arXiv:2101.03564*, 2021.
- [11] Stig Olav Settemsdal, Ben Bishop, et al. When to go with cloud or edge computing in offshore oil and gas. In *SPE Offshore Europe Conference and Exhibition*. Society of Petroleum Engineers, 2019.
- [12] Cristina Alcaraz and Sherali Zeadally. Critical control system protection in the 21st century. *Computer*, 46(10):74–83, 2013.
- [13] Ioannis Stelliou, Panayiotis Kotzanikolaou, Mihalys Psarakis, Cristina Alcaraz, and Javier Lopez. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials*, 20(4):3453–3495, 2018.
- [14] M Nygaard and S Mukhopadhyay. Dragonstone strategy kickoff report. Technical report, Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), 2020.
- [15] Hansong Xu, Wei Yu, David Griffith, and Nada Golmie. A survey on industrial internet of things: A cyber-physical systems perspective. *IEEE Access*, 6:78238–78259, 2018.
- [16] Planete Energies. Offshore oil and gas production, 2015.
- [17] Ruth Olurounbi. Nigeria in talks with shell over onshore divestment plans, 2021.
- [18] Hellenic Shipping News. Nigeria confirms it is in talks with shell over sale of onshore oil assets, 2021.
- [19] Equinor. Equinor sells its us onshore assets in the bakken, 2021.
- [20] Piotr Ciepiela. Digitization and cyber disruption in oil and gas, 2016.

- [21] Ben Dickinson, Mario Chiock, et al. Guest editorial: Countering security issues in the digital world. *Journal of Petroleum Technology*, 71(06):14–15, 2019.
- [22] Space Rogue. Tilting it sideways, 2016.
- [23] Robert Lee, Michael Assante, and Tim Conway. Media report of the baku-tbilisi-ceyhan (btc) pipeline cyber attack, 2014.
- [24] Jordan Robertson and Michael Riley. Mysterious '08 turkey pipeline blast opened new cyberwar, 2014.
- [25] Collin Eaton. Hacked part 1: As cyberattacks become more sophisticated, energy industry's controls provide an alluring target, 2018.
- [26] Ponemon Institute. The state of cybersecurity in the oil & gas industry: United states, 2017.
- [27] David Sanger, Clifford Krauss, and Nicole Perlroth. Cyberattack forces a shutdown of a top us pipeline, 2021.
- [28] Joe R Reeder and Cadet Tommy Hall. Cybersecurity's pearl harbor moment: Lessons learned from the colonial pipeline ransomware attack. 2021.
- [29] Kyoung-Dae Kim and Panganamala R Kumar. Cyber-physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(Special Centennial Issue):1287–1308, 2012.
- [30] Maryna Krotofil and Dieter Gollmann. Industrial control systems security: What is happening? In *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, pages 670–675. IEEE, 2013.
- [31] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2011.
- [32] Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, and Ramesh Karri. The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5):1039–1057, 2016.
- [33] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2015.
- [34] Wazir Zada Khan, Mohammed Y Aalsalem, Muhammad Khurram Khan, Md Shohrab Hossain, and Mohammed Atiquzzaman. A reliable internet of things based architecture for oil and gas industry. In *2017 19th International conference on advanced communication Technology (ICACT)*, pages 705–710. IEEE, 2017.
- [35] Naoum Sayegh, Ali Chehab, Imad H Elhadj, and Ayman Kayssi. Internal security attacks on scada systems. In *2013 Third International Conference on Communications and Information Technology (ICCIT)*, pages 22–27. IEEE, 2013.
- [36] Sajid Nazir, Shushma Patel, and Dilip Patel. Assessing and augmenting scada cyber security: A survey of techniques. *Computers & Security*, 70:436–454, 2017.
- [37] Deval Bhamare, Maede Zolanvari, Aiman Erbad, Raj Jain, Khaled Khan, and Nader Meskin. Cybersecurity for industrial control systems: A survey. *Computers & Security*, 89:101677, 2020.
- [38] Bill Miller and Dale Rowe. A survey scada of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology*, pages 51–56, 2012.
- [39] Jairo Giraldo, Esha Sarkar, Alvaro A Cardenas, Michail Maniatakos, and Murat Kantarcioglu. Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design & Test*, 34(4):7–17, 2017.
- [40] Sean McBride, Jeffery Ashcraft, and Nathan Belk. Overload: Critical lessons from 15 years of ics vulnerabilities, 2016.
- [41] Dragos Inc. Global oil and gas cyber threat perspective, 2019.
- [42] Francis Lobo. Upstream oil & gas cyber risk: Insurance technical review, 2019.
- [43] Anil Lamba. Protecting 'cybersecurity & resiliency' of nation's critical infrastructure—energy, oil & gas. *International Journal of Current Research*, 10:76865–76876, 2018.
- [44] Emily Darko. Short guide summarising the oil and gas industry lifecycle for a non-technical audience. *London: Overseas Development Institute*, 2014.
- [45] Ann Scarborough Bull and Milton S Love. Worldwide oil and gas platform decommissioning: a review of practices and reefing options. *Ocean & coastal management*, 168:274–306, 2019.
- [46] Alexander Polyakov and Matheu Geli. Sap cybersecurity for oil and gas. Technical report, ERP Scan, 2015.

- [47] Håvard Devold. Oil and gas production handbook. 2006.
- [48] A Mittal, A Slaughter, and P Zonneveld. Protecting the connected barrels: Cybersecurity for upstream oil and gas. *Deloitte Insights, London, UK, Tech. Rep.*, 2017.
- [49] Xiaodao Chen, Dongmei Zhang, Yuewei Wang, Lizhe Wang, Albert Zomaya, and Shiyan Hu. Offshore oil spill monitoring and detection: Improving risk management for offshore petroleum cyber-physical systems. In *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 841–846. IEEE, 2017.
- [50] Jaime HuiChoo Tan, Brian Roberts, Prabakaran Sundararaju, Christophe Sintive, Laurent Facheris, Joel Vanden Bosch, Virginie Lehning, and Mathew Pegg. Transforming offshore oil and gas production platforms into smart unmanned installations. In *Offshore Technology Conference Asia*. OnePetro, 2020.
- [51] Utheswaran Krishna Moorthy, Denys Anding, Chieh Lung Ng, Sobri Songli, Sahlan Sahak, and Mohd Hafiz Baharudin. Alternative method to supply pneumatic air to an unmanned platform, in the event of the platform’s instrument gas system is on downtime. In *SPE Annual Technical Conference and Exhibition*. OnePetro, 2020.
- [52] MF Mahmoud Radwan. Safe and economic attractive rigless operations using a digital slickline in unmanned platform with low structure loads and spacing. In *Abu Dhabi International Petroleum Exhibition & Conference*. OnePetro, 2020.
- [53] Justin Okpala, Oluwasegun Adedokun, Adagogo Jaja, Olubukola Olubukola, Emeka Ogugua, Joseph Olayomi, Inegbenose Aitokhuehi, Peters Korede, Kunle Awonuga, and Obor Eruvbentine. Enabling reservoir management excellence through real time surveillance of an unmanned onshore gas-condensate field platform. In *SPE Nigeria Annual International Conference and Exhibition*. OnePetro, 2020.
- [54] Jan Erik Vinnem. Assessment of risk tolerance for future autonomous offshore installations. *Safety science*, 134:105059, 2021.
- [55] Anna Isabella Thomassen Frostad, Thomas Singer, Linda Fløttum, Trygve Andreas Rikheim, Robin Balas, Svein Audun Haaheim, et al. Unmanned full processing platforms; using subsea technology as enabler. In *Offshore Technology Conference*. Offshore Technology Conference, 2020.
- [56] Oil & Gas Authority. Analysis of ukcs operating costs in 2016, 2017.
- [57] Fan Zhang, Hansaka Angel Dias Edirisinghe Kodituwakku, J Wesley Hines, and Jamie Coble. Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, 15(7):4362–4369, 2019.
- [58] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. *Journal of Network and Computer Applications*, 149:102481, 2020.
- [59] Christian Mudrak. *Subsea production systems-A review of components, maintenance and reliability*. PhD thesis, University of Leoben, 2016.
- [60] Eirini Anthi, Amir Javed, Omer Rana, and George Theodorakopoulos. Secure data sharing and analysis in cloud-based energy management systems. In *Cloud Infrastructures, Services, and IoT Systems for Smart Cities*, pages 228–242. Springer, 2017.
- [61] Namje Park and Namhi Kang. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. *Sensors*, 16(1):20, 2016.
- [62] Joe Weiss. What the lack of cyber security of process sensors means, 2019.
- [63] Helen K White, Pen-Yuan Hsing, Walter Cho, Timothy M Shank, Erik E Cordes, Andrea M Quattrini, Robert K Nelson, Richard Camilli, Amanda WJ Demopoulos, Christopher R German, et al. Impact of the deepwater horizon oil spill on a deep-water coral community in the gulf of mexico. *Proceedings of the National Academy of Sciences*, 109(50):20303–20308, 2012.
- [64] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys (CSUR)*, 51(4):1–36, 2018.
- [65] Mazen Azzam, Liliana Pasquale, Gregory Provan, and Bashar Nuseibeh. Grounds for suspicion: Physics-based early warnings for stealthy attacks on industrial control systems. *arXiv preprint arXiv:2106.07980*, 2021.
- [66] James M Taylor and Hamid R Sharif. Security challenges and methods for protecting critical infrastructure cyber-physical systems. In *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, pages 1–6. IEEE, 2017.
- [67] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, and Alberto Coen-Porisini. Reato: Reacting to denial of service attacks in the internet of things. *Computer Networks*, 137:37–48, 2018.

- [68] F Hacquebord and C Pernet. Drilling deep: A look at cyberattacks on the oil and gas industry. *Trend Micro Research*, 2019.
- [69] Mordor Intelligence. Subsea systems market - growth, trends, covid-19 impact, and forecasts (2021 - 2026), 2021.
- [70] Research and Market. Global distributed control systems (dcs) market in the oil and gas industry 2019-2023. Technical report, Research and Market, 2019.
- [71] David Kravets. Feds: Hacker disabled offshore oil platforms' leak-detection system, 2009.
- [72] Piotr Ciepiela, Bala V Venkateshwaran, et al. Evolution of cyber threats and the development of new security architecture. In *22nd World Petroleum Congress*. World Petroleum Congress, 2017.
- [73] Science X. Chevron says hit by stuxnet virus in 2010, 2012.
- [74] Rahat Masood. Assessment of cyber security challenges in nuclear power plants security incidents, threats, and initiatives. *Cybersecurity and Privacy Research Institute the George Washington University*, 2016.
- [75] Bernard Brode. 7 cyber threat actors to watch for in 2021, 2021.
- [76] A Stacey, M Birkinshaw, and JV Sharp. Life extension issues for ageing offshore installations. In *International Conference on Offshore Mechanics and Arctic Engineering*, volume 48227, pages 199–215, 2008.
- [77] M Rosner, P Herve, K Moore, et al. Using a cognitive analytic approach to enhance cybersecurity on oil and gas ot systems. In *Offshore Technology Conference*. Offshore Technology Conference, 2017.
- [78] Hadi Almusaher, Gulzar Alam, et al. How feasible moving target defense is within ics environment. In *International Petroleum Technology Conference*. International Petroleum Technology Conference, 2020.
- [79] Rachel Adams-Heard, David Wethe, and Kevin Crowley. Turning oil wells back on is trickier than shutting them off, 2020.
- [80] Doug Walser. Production restarts: Fiscal, technical issues define operator strategies in restarting shut-in wells, 2021.
- [81] Offshore Technology. The longest standing fixed offshore platforms, 2019.
- [82] Silvia Tham. Exploring the growth of the fpso industry, 2019.
- [83] Oil and Gas IQ. 10 reasons why fpsos are the future of oil and gas, 2019.
- [84] Offshore Energy. Samsung to build largest fpso in the world, 2013.
- [85] Karsten Friis, Lilly Pijnenburg Muller, and Lars Gjesvik. Cyber-weapons in international politics: Possible sabotage against the norwegian petroleum sector. *NUPI Report*, 2018.
- [86] Alireza Esfahani, Georgios Mantas, Rainer Maticsek, Firooz B Saghezchi, Jonathan Rodriguez, Ani Bicaku, Silia Maksuti, Markus G Tauber, Christoph Schmittner, and Joaquim Bastos. A lightweight authentication mechanism for m2m communications in industrial iot environment. *IEEE Internet of Things Journal*, 6(1):288–296, 2017.
- [87] Jangirala Srinivas, Ashok Kumar Das, Mohammad Wazid, and Neeraj Kumar. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things. *IEEE Transactions on Dependable and Secure Computing*, 17(6):1133–1146, 2018.
- [88] Ayman Al-Issa et al. Protecting the digital oil field from emerging cyber threats. In *Abu Dhabi International Petroleum Conference and Exhibition*. Society of Petroleum Engineers, 2012.
- [89] Mohammad Aljubran, Mohammed Al-Ghazal, Viranchi Vedpathak, et al. Integrated cybersecurity for modern information control models in oil and gas operations. In *SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility*. Society of Petroleum Engineers, 2018.
- [90] Felix O Olowononi, Danda B Rawat, and Chunmei Liu. Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps. *IEEE Communications Surveys & Tutorials*, 2020.
- [91] Mohammad Sayad Haghighi, Faezeh Farivar, and Alireza Jolfaei. A machine learning-based approach to build zero false-positive ipss for industrial iot and cps with a case study on power grids security. *IEEE Transactions on Industry Applications*, 2020.
- [92] Eirini Anthi, Lowri Williams, Amir Javed, and Pete Burnap. Hardening machine learning denial of service (dos) defences against adversarial attacks in iot smart home networks. *computers & security*, page 102352, 2021.
- [93] Louis Wehenkel. Machine learning approaches to power-system security assessment. *IEEE Expert*, 12(5):60–72, 1997.

- [94] Sumeet Dua and Xian Du. *Data mining and machine learning in cybersecurity*. CRC press, 2016.
- [95] Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security*, pages 355–366, 2011.
- [96] Yun-Gui Zhang, Wei Zhang, Xiang-Rong Xue, and Xiao-Jun Yang. Scada intrusion detection system based on self-learning semi-supervised one-class support vector machine. *Metallurgical Industry Automation*, 37(2):1–5, 2013.
- [97] SLP Yasakethu and J Jiang. Intrusion detection via machine learning for scada system protection. In *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*, pages 101–105, 2013.
- [98] Justin M Beaver, Raymond C Borges-Hink, and Mark A Buckner. An evaluation of machine learning methods to detect malicious scada communications. In *2013 12th International Conference on Machine Learning and Applications*, volume 2, pages 54–59. IEEE, 2013.
- [99] Leandros A Maglaras and Jianmin Jiang. Intrusion detection in scada systems using machine learning techniques. In *2014 Science and Information Conference*, pages 626–631. IEEE, 2014.
- [100] Raymond C Borges Hink, Justin M Beaver, Mark A Buckner, Tommy Morris, Uttam Adhikari, and Shengyi Pan. Machine learning for power system disturbance and cyber-attack discrimination. In *2014 7th International symposium on resilient control systems (ISRCs)*, pages 1–8. IEEE, 2014.
- [101] Noam Erez and Avishai Wool. Control variable classification, modeling and anomaly detection in modbus/tcp scada systems. *International Journal of Critical Infrastructure Protection*, 10:59–70, 2015.
- [102] Vojtech Franc, Michal Sofka, and Karel Bartos. Learning detector of malicious network traffic from weak labels. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, pages 85–99. Springer, 2015.
- [103] Patric Nader, Paul Honeine, and Pierre Beausery. Detection of cyberattacks in a water distribution system using machine learning techniques. In *2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, pages 25–30. IEEE, 2016.
- [104] Kevin Leahy, R Lily Hu, Ioannis C Konstantakopoulos, Costas J Spanos, and Alice M Agogino. Diagnosing wind turbine faults using machine learning techniques applied to operational data. In *2016 IEEE International Conference on Prognostics and Health Management (ICPHM)*, pages 1–8. IEEE, 2016.
- [105] Alfonso Valdes, Richard Macwan, and Matthew Backes. Anomaly detection in electrical substation circuits via unsupervised machine learning. In *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)*, pages 500–505. IEEE, 2016.
- [106] Kyriakos Stefanidis and Artemios G Voyiatzis. An hmm-based anomaly detection approach for scada systems. In *IFIP International Conference on Information Security Theory and Practice*, pages 85–99. Springer, 2016.
- [107] Karel Bartos, Michal Sofka, and Vojtech Franc. Optimized invariant representation of network traffic for detecting unseen malware variants. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pages 807–822, 2016.
- [108] Pu Zeng and Peng Zhou. Intrusion detection in scada system: A survey. In *Intelligent Computing and Internet of Things*, pages 342–351. Springer, 2018.
- [109] Youbiao He, Gihan J Mendis, and Jin Wei. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid*, 8(5):2505–2516, 2017.
- [110] Sasanka Potluri, Navin Francis Henry, and Christian Diedrich. Evaluation of hybrid deep learning techniques for ensuring security in networked control systems. In *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8. IEEE, 2017.
- [111] Anastasis Keliris, Hossein Salehghaffari, Brian Cairl, Prashanth Krishnamurthy, Michail Maniatakos, and Farshad Khorrami. Machine learning-based defense against process-aware attacks on industrial control systems. In *2016 IEEE International Test Conference (ITC)*, pages 1–10. IEEE, 2016.
- [112] Yi Zhang, Marija D Ilić, and Ozan K Tonguz. Mitigating blackouts via smart relays: A machine learning approach. *Proceedings of the IEEE*, 99(1):94–118, 2010.
- [113] Imtiaz Ullah and Qusay H Mahmoud. A hybrid model for anomaly-based intrusion detection in scada networks. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 2160–2167. IEEE, 2017.
- [114] Irfan A Siddavatam, S Satish, W Mahesh, and Faruk Kazi. An ensemble learning for anomaly identification in scada system. In *2017 7th International Conference on Power Systems (ICPS)*, pages 457–462. IEEE, 2017.

- [115] Thiago Alves, Rishabh Das, and Thomas Morris. Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. *IEEE Embedded Systems Letters*, 10(3):99–102, 2018.
- [116] Oliver Eigner, Philipp Kreimel, and Paul Tavorato. Detection of man-in-the-middle attacks on industrial control networks. In *2016 International Conference on Software Security and Assurance (ICSSA)*, pages 64–69. IEEE, 2016.
- [117] Maede Zolanvari, Marcio A Teixeira, Lav Gupta, Khaled M Khan, and Raj Jain. Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal*, 6(4):6822–6834, 2019.
- [118] Seungoh Choi, Jeong-Han Yun, and Sin-Kyu Kim. A comparison of ics datasets for security research based on attack paths. In *International Conference on Critical Information Infrastructures Security*, pages 154–166. Springer, 2018.
- [119] Thomas Morris and Wei Gao. Industrial control system traffic data sets for intrusion detection research. In *International Conference on Critical Infrastructure Protection*, pages 65–78. Springer, 2014.
- [120] Antoine Lemay and José M Fernandez. Providing {SCADA} network data sets for intrusion detection research. In *9th Workshop on Cyber Security Experimentation and Test ({CSET} 16)*, 2016.
- [121] Jonathan Goh, Sridhar Adepu, Khurum Nazir Junejo, and Aditya Mathur. A dataset to support research in the design of secure water treatment systems. In *International conference on critical information infrastructures security*, pages 88–99. Springer, 2016.
- [122] Nicholas R Rodofile, Thomas Schmidt, Sebastian T Sherry, Christopher Djamaludin, Kenneth Radke, and Ernest Foo. Process control cyber-attacks and labelled datasets on s7comm critical infrastructure. In *Australasian Conference on Information Security and Privacy*, pages 452–459. Springer, 2017.
- [123] ICS Lab. 4sics ics lab pcap files, 2015.
- [124] Dale Peterson and Reid Wightman. Digital bond s4x15 ics village ctf pcap files, 2015.
- [125] DEFCON23. compilation of ics pcap files indexed by protocol, 2015.
- [126] Mirjana D Stojanović and Slavica V Boštjančič Rakas. Building industrial scale cyber security experimentation testbeds for critical infrastructures. In *Cyber Security of Industrial Control Systems in the Future Internet Environment*, page 215. IGI Global, 2020.